Principali informazioni sull'insegnamento	
Titolo insegnamento	Crittografia
Corso di studio	Laurea magistrale in Sicurezza Informatica
Crediti formativi	6
Denominazione inglese	Cryptography
Obbligo di frequenza	-
Lingua di erogazione	Italiano

Docente responsabile	Nome Cognome	Indirizzo mail
	Costantina Caruso	costantina.caruso@uniba.it

Dettaglio credi formativi	Ambito disciplinare	SSD	Crediti
	Informatica	Inf/01	6

Modalità di erogazione	
Periodo di erogazione	Semestre primo
Anno di corso	Primo
Modalità di erogazione	Lezioni frontali (4 CFU) ed esercitazioni guidate (2 CFU) Lezioni frontali per 62 ore (32 ore lezioni teoriche e 30 ore di esercitazioni guidate)

Organizzazione della didattica	
Ore totali	62 + 88 = 150 corrispondenti a 6 CFU
Ore di corso	62
Ore di studio individuale	68 corrispondenti alle lezioni teoriche 20 corrispondenti alle esercitazioni guidate

Calendario	
Inizio attività didattiche	
Fine attività didattiche	

Syllabus	
Prerequisiti	• *Conoscenze di matematica discreta, algebra e programmazione, del linguaggio di programmazione C*
Risultati di apprendimento previsti (declinare rispetto ai Descrittori di Dublino) (si raccomanda che siano coerenti con i risultati di apprendimento del CdS, compreso i risultati di apprendimento trasversali)	• *Conoscenza e capacità di comprensione* Conoscenza e comprensione di principi, algoritmi e protocolli crittografici; conoscenza e comprensione degli utilizzi della crittografia. • *Conoscenza e capacità di comprensione applicate*

	Capacità di valutare il grado di sicurezza di algoritmi e protocolli informatici; capacità di valutare il grado di sicurezza di sistemi informatici che usano strumenti crittografici. Analisi, integrazione e utilizzo di strumenti crittografici nello sviluppo e gestione dei sistemi software per la protezione proattiva dei dati e delle informazioni • *Autonomia di giudizio* Lo studente sarà in grado di valutare la qualità della soluzione crittografica usata rispetto alla tipologia di utilizzo, al livello di protezione richiesta in base alla quantità di potenza computazionale a cui un potenziale avversario può avere accesso, e rispetto all'intervallo di tempo presunto di utilizzo del sistema • *Abilità comunicative* Lo studente acquisirà abilità comunicative e adeguata appropriatezza espressiva per un registro di comunicazione non tecnico, adatto anche ad interlocutori non esperti del settore. Queste abilità vengono acquisite nelle discussioni con il docente e con i colleghi del corso tramite discussioni e riflessioni sulle comuni applicazioni crittografiche. • *Capacità di apprendere* Lo studente avrà la capacità di seguire l'evoluzione tecnologica di algoritmi e protocolli crittografici e di adeguare autonomamente il proprio livello di preparazione. Lo studente sarà di consultare materiale bibliografico tradizionale o disponibile su Internet. Le linee guida dell'apprendimento sono fornite tramite slide del docente, le esercitazioni fornite, articoli di ricerca o di contenuto tecnico discussi in appositi momenti di svolgimento del corso.
Contenuti di insegnamento	• Introduzione alla crittografia • Utilizzi della crittografia: confidenzialità, integrità, autenticazione, non ripudio • Principi di teoria dell'informazione e teoria dei

	numeri • Crittosistemi • Crittosistemi monoalfabetici e polialfabetici, a pacchetto e a flusso • Cifrario di Vernam e cifrario di Cesare • Crittosistemi a chiave privata, DES, TDES e AES • Crittosistemi a chiave pubblica, doppio lucchetto, Diffie-Hellmann, RSA, ElGamal • Firma digitale • Funzioni Hash • Introduzione ai protocolli crittografici • Protocolli crittografici di base: scambio di chiavi, autenticazione, Needam-Schroeder, Kerberos, One Time Password, Secret Splitting, Marcatura temporale di un documento • Protocolli crittografici avanzati: firma cieca, denaro elettronico, crittomonete • Applicazioni della crittografia: public key infrastructure, PGP, blockchain,bitcoin, KDC

Programma	
Testi di riferimento	A.J. Menezes, P.C. van Oorschot, S.A. Vanstone; Handbook of Applied Cryptography; CRC Press Slide docente
Note ai testi di riferimento	
Metodi didattici	Lezioni frontali Esercitazioni guidate
Metodi di valutazione (indicare almeno la tipologia scritto, orale, altro)	L’esame consiste in una prova orale.
Criteri di valutazione (per ogni risultato di apprendimento atteso su indicato, descrivere cosa ci si aspetta lo studente conosca o sia in grado di fare e a quale livello al fine di dimostrare che un risultato di apprendimento è stato raggiunto e a quale livello)	Si richiede che lo studente sia in grado di analizzare un protocollo crittografico rispetto ai requisiti di confidenzialità, autenticità, integrità e non ripudio nella sicurezza dei dati e delle informazioni. Lo studente inoltre deve essere in grado di valutare la complessità computazionale di un algoritmo crittografico rispetto alle operazioni di di cifratura e di decifratura e il livello di sicurezza dell’algoritmo stesso. Infine lo studente deve essere in grado di individuare vantaggi e svantaggi dei protocolli di cifratura rispetto alle applicazioni previste
Altro	